課題 4 (RSA で暗号化されたファイルの復号) について

野呂 正行

December 12, 2011

1 課題 4 について

課題 4 は, RSA 暗号で暗号化されたファイルの復号である. 暗号化されたファイルは,

e	n	A_1	A_2	$\ldots$	A_m

という形をしている. ここで, e, n, A_i は「整数」を表すバイト列である. 「整数」は, 大きな正整数をバイト列として表現するためのデータ型で,

l	c_0	$\ldots$	c_{l-1}

という形をしている. l, c_i は 1 バイト正整数で,

$$c_0 \times 256^{l-1} + \cdots + c_{l-2} \times 256 + c_{l-1}$$

を表している. (n, e) は公開鍵であり, 各 A_i は, 平文 (文字列) を, ある長さに区切り, n 未満の整数と見たものを e 乗して n で割った余りを表している. よって, 復号するには

1. 上記フォーマットの「整数」を順に正しく読みとる.

   これは, ファイルを読み込みモードで open し, 一バイト読むと, 先頭の「整数」を構成するバイト数がわかるので, 各バイトを読みだし, その「整数」が表す整数を復元する, という操作を, ファイルか空になるまで繰り返せばよい. 得られた整数列は例えばリストとして保存する.

2. $n = pq$ (p, q は素数) と素因数分解する.

   これは `pari(factor,n)` で行う.

3. $n' = (p-1)(q-1)$ に対し, $ed \equiv 1 \bmod n'$ となる正整数

   d の計算は, 授業で説明したように 2 通りの方法が考えられる. これは, $de + kn' = 1$ を満たす d, k を求めることになり, 一般には互除法で行うが, 本課題の場合 $e = 65537$ が小さいので, $kn' \equiv 1 \bmod e$ を満たす k を単純な繰り返しで求めれば, それから d が逆算できる. 余裕がある人は, 任意の場合に使える拡張ユークリッド互除法を実装してみてほしい.

4. d を求め, $D_i = A_i^d \bmod n$ を計算する.

   各 D_i を $D_i = c_0 \times 256^{m-1} + \cdots + c_{m-1}$ と 256 進展開し, バイト列 $(c_0, \ldots, c_{m-1})$ に直す.

   べき乗剰余を効率よく求める関数, および, 整数を 256 進展開する関数を書く必要がある. これは p114 の `encode(X,A,N)` を $X = A_i$,$A = d$,$N = n$ で呼び出せばよい.

5. 得られたバイト列を順にファイルに書き出す.

   これは, ファイルを書き出しモードで open し, 一バイトずつ書き出し, ファイルを close すればよい.

という操作を行えばよい. まず, 1. のファイルからの整数の読み込み関数を書くのが先決である. テスト用に, `http://orange2.math.kobe-u.ac.jp/HOME/noro/` の計算数学 I のページに `int_test` というファイルを置いた. これを読み出して 12345678987654321 が得られれば OK である. `longint_test` の方は整数列の読み込みテスト用である. 10^i がたくさん出て来れば OK である.

2　ファイル名について

`open_file(ファイル名,"rb")` でファイルを開く場合, ファイル名は絶対パスで与える必要がある. ここで,「絶対パス」とは, ファイルの位置を特定するための名前である. すなわち, ルート (根) からスタートして, ディレクトリ (フォルダ) をたどって目的のファイルにたどりつくまでの経路を

`/ディレクトリ 1/ディレクトリ 2/.../ファイル`

と表示するのが絶対パスである. これを指定しないとファイルが開けられない.

さらにややこしいことに, Finder などで表示される名前は, 拡張子 (`.rr` など) が表示されない場合がある. この場合も, 拡張子までつけた完全なファイル名を入れないとファイルは開けられない.

以下では, Mac 上でファイルの絶対パス名を知る方法について述べる.

1. Finder から目的ファイルがあるディレクトリを開く.
2. 目的のファイルをシングルクリックして,「ファイル → 情報を見る」
3. 「場所」を見れば, ファイルのおかれたディレクトリが分かる.
4. 「名前と拡張子」を開けると, 拡張子を含んだ完全な名前が分かる.
5. 3. と 4. を繋いだものが, ファイルの絶対パス名である.

   (`/Users/noro/Desktop/encode.rr` など).

ちなみに, `X11` を起動し, `xterm` から, `pwd` (現在のディレクトリの表示), `ls` (ディレクトリにあるファイル名の表示) を使ってもできる.